安全性評価の手順

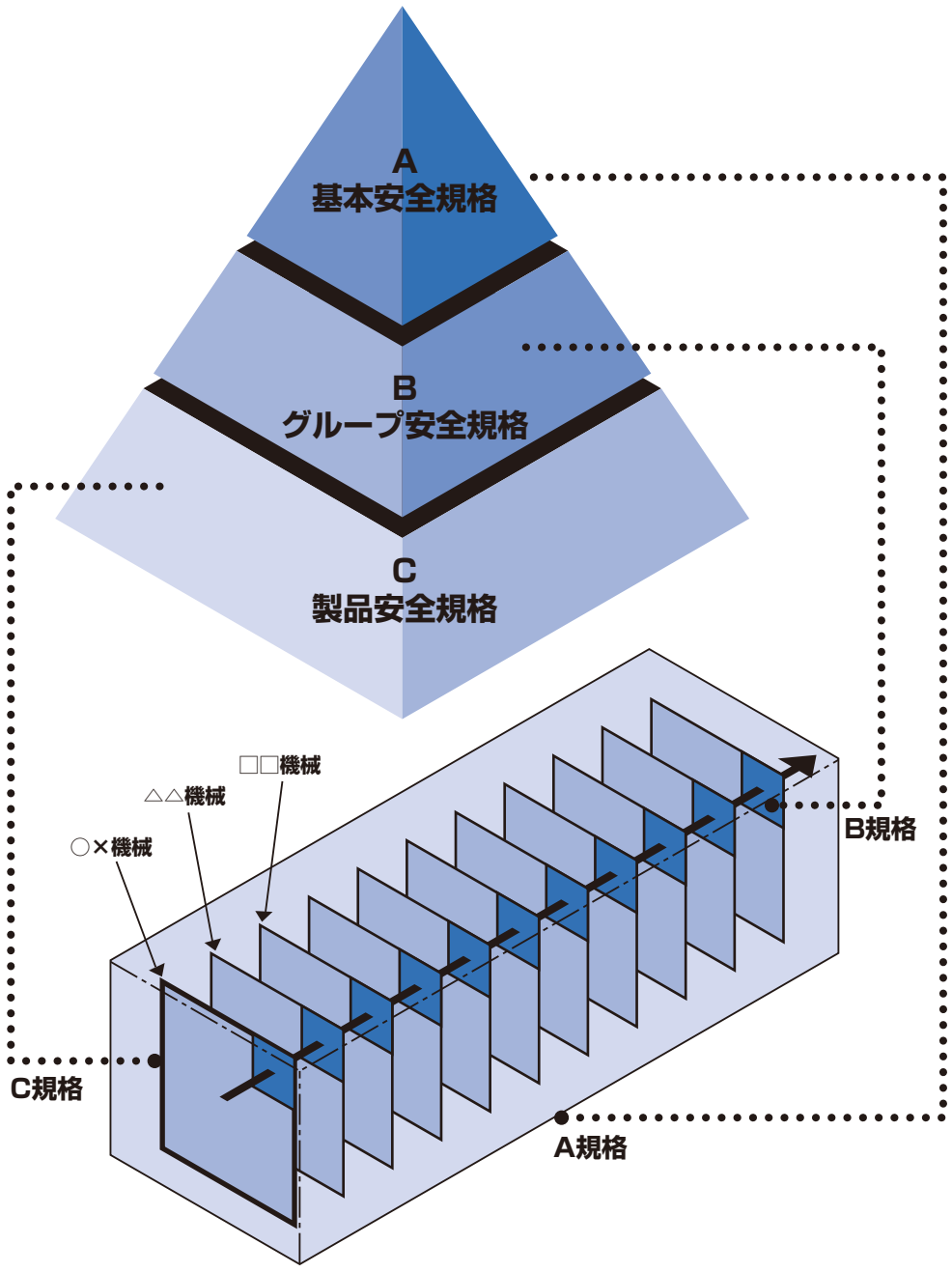
■A、B、C規格の使い分け

機械類の設計を行う上で、その安全性を確認するために、最初に適用規格を決定する必要があります。先に紹介したとおり、基本安全規格のA規格、グループ安全規格のB規格、製品安全規格のC規格によって体系づけられており、原則として各々の関係は、A規格の要求に基づいてB規格が制御や工程など機械共通の安全部分を、さらにA規格とB規格の要求に基づいてC規格が個々機械設備の安全部分を具体的に規定していくものとされています。

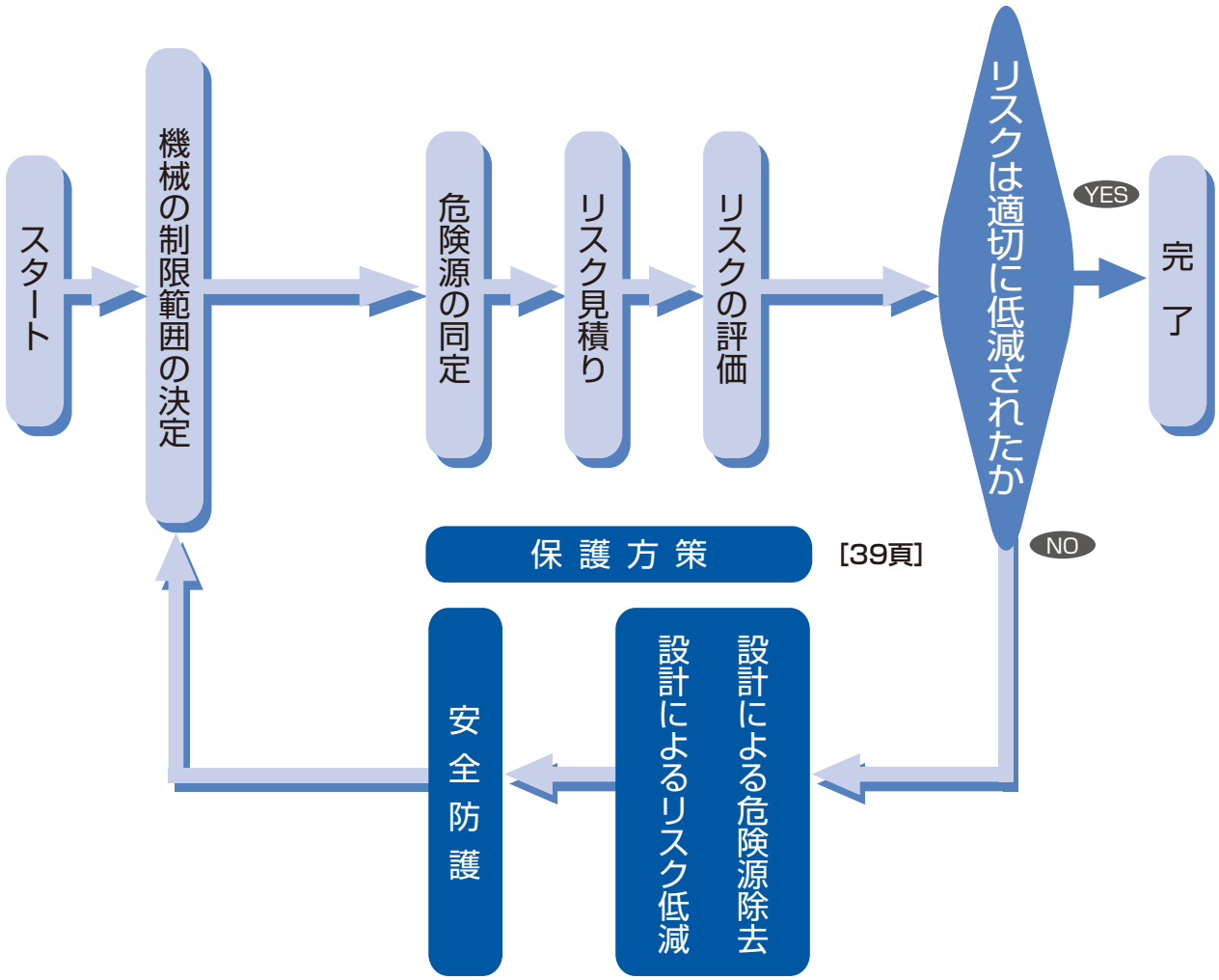
したがって、機械類の適用規格を決定する場合、利用可能なC規格が存在すればそれを適用するのが早道ですが、実際には全ての機械類に対してC規格が整備されているわけではありません。

また、日々進歩する機械設備の高性能化や多様化により、既存のC規格の適用範囲を超える場合があるのも実情です。

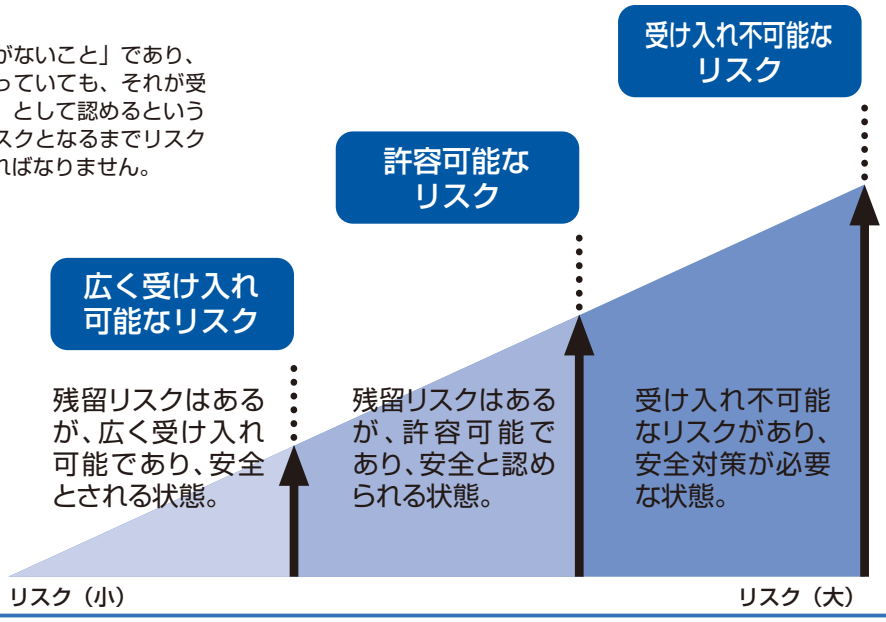
このように利用可能なC規格が存在しない場合、また既存のC規格では安全性の評価に対して不十分な場合、A規格やB規格で要求される安全原則に基づいて評価確認作業を進めることが必要となります。



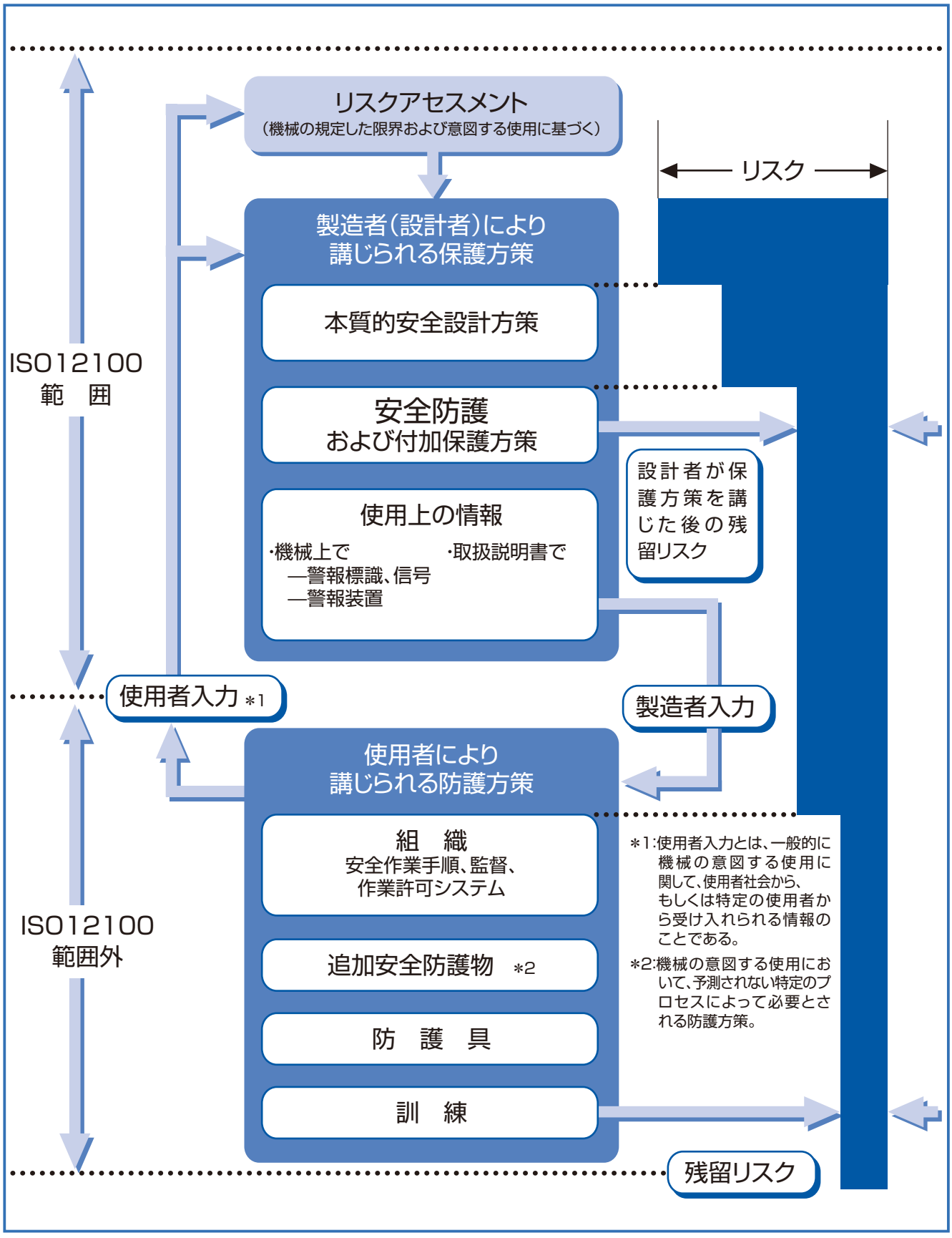
リスクアセスメントのフロー



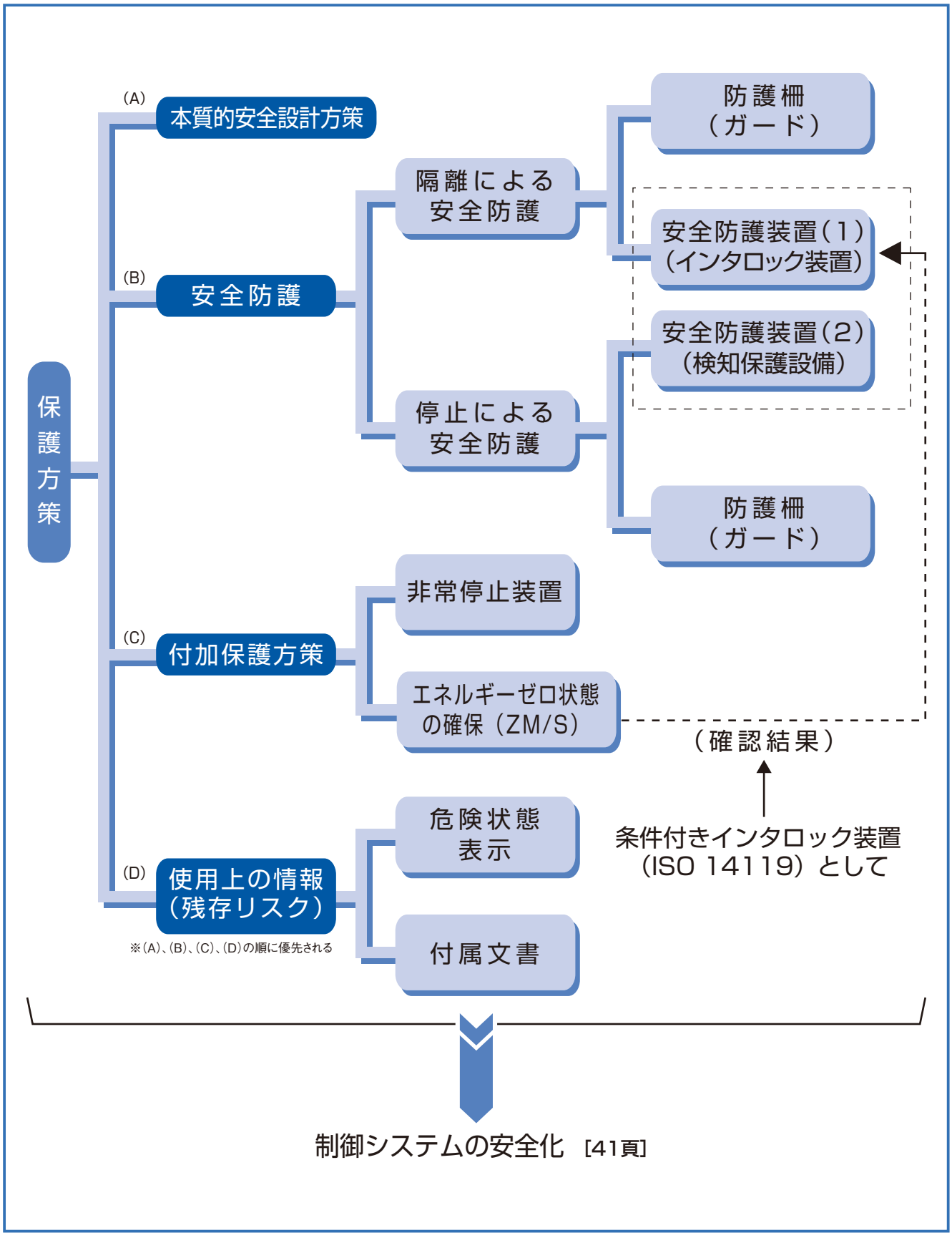
安全とは「受け入れ不可能なリスクがないこと」であり、別の言い方をすれば残留リスクが残っていても、それが受け入れ可能なリスクであれば「安全」として認めるということです。少なくとも許容可能なリスクとなるまでリスク低減のための安全方策を実施しなければなりません。



ISO12100/JIS B 9700の応用範囲(適用する保護方策の階層)



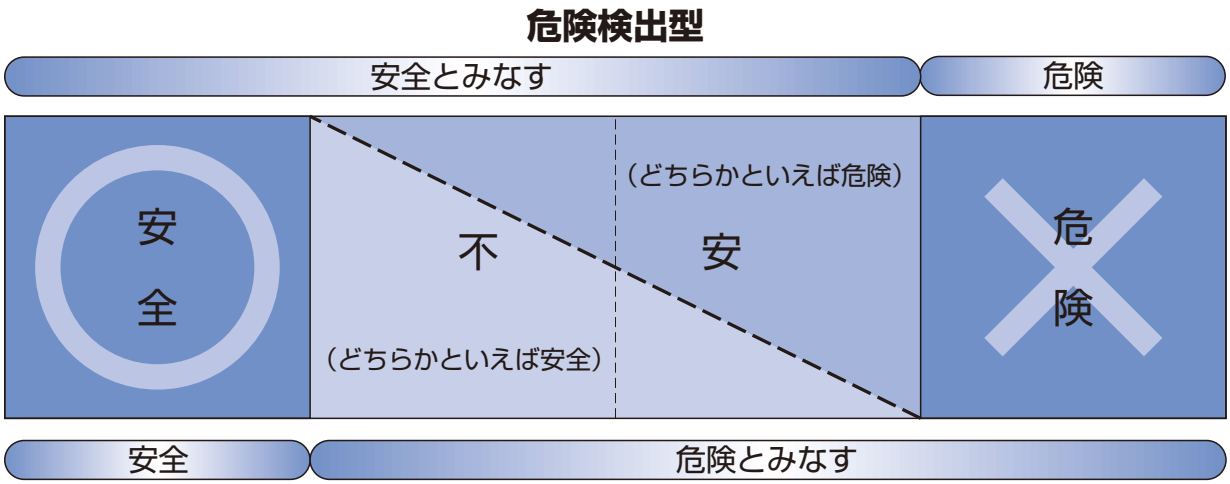
保護方策


保護方策
(A)
本質的安全設計方策
(B)
安全防護
(C)
付加保護方策
(D)
使用上の情報
(残存リスク)
※(A)、(B)、(C)、(D)の順に優先される
隔離による
安全防護
停止による
安全防護
防護柵
(ガード)
安全防護装置(1)
(インタロック装置)
安全防護装置(2)
(検知保護設備)
防護柵
(ガード)
非常停止装置
エネルギーゼロ状態
の確保(ZM/S)
危険状態
表示
付属文書
(確認結果)
条件付きインタロック装置
(ISO 14119)として
制御システムの安全化 [41頁]

■保護方策の基本的な考え方

機械の安全化を図るには、危険状態を検出して機械の運転を停止させるのではなく、作業者のミスや機械の故障を前提とし、安全が確認できる場合のみ機械の運転を許可する安全確認型を基本としなければなりません。

■危険検出型と安全確認型



危険検出型

危険状態の証拠を確認 → 情報伝達(エネルギー) → 運転停止

危険状態の証拠が確認(検出)された時、情報を伝達し(エネルギーを出して)、運転を停止させる。
(確認、伝達のどこかが故障すると、危険状態になっても運転は停止しない)

安全確認型

安全状態の証拠を確認 → 情報伝達(エネルギー) → 運転許可

安全状態の証拠が確認(検出)された時、情報を伝達し(エネルギーを出して)、運転を許可する。
(確認、伝達のどこかが故障すると運転できない)